Layer 2 Deployment

Where to deploy Alongside?

As Ethereum blockspace becomes more in demand, the fees will not allow our users to interact with our application. This has been an issue on people's minds in recent years, and so many teams took it upon themselves to scale Ethereum and devise competitor L1s to capture blockspace market share. These teams have built several solutions, and each of these has different properties, security and scalability guarantees, different levels of adoption, and technological adoption. This resource clarifies the current state of affairs in the L2 ecosystem and where Alongside fits into the picture.

Alongside Requirements

Security and decentralization need to be the foremost priority to bring crypto market indexes to the world. The network we settle on will be responsible for the safety of the index tokens that will represent the underlying assets of the index held by decentralized/centralized custodians on their respective chains. We also need mass scalability for the long term if we want to make this a product that anyone can use to get broad exposure to cryptocurrencies and other various on-chain native assets.

List of relevant requirements and concerns:

- low cost
- security
- scalability
- decentralization of infrastructure
- good tooling
- value alignment
- incentives

- interoperability
    - liquidity
    - access to DeFi primitives
    - core infrastructure
        - multisigs
        - wallets
        - CEXs
        - bridges
        - DAO tooling
- Flexibility
    - the ability to pivot to a better solution once deployed
    - migration in case of emergency (chain halts forever, liquidity stuck, hack, etc.)

Considering the requirements, let's unpack all of these concerns sequentially and explain the discredited solutions.

Low cost

Our application needs to be affordable to as many people as possible to get broad market exposure quickly. As it stands, 99.9% of the world is priced out of using most blockchains. We can discard the Ethereum mainnet as a viable solution due to the low-cost requirement.

	Before EIP-4844 (Send ETH)	Before EIP-4844 (Swap tokens)	After EIP-4844 (Send ETH)	After EIP-4844 (Swap tokens)
Boba Network	$0.06	$0.40	$0.0006	$0.0040
Loopring	$0.07	$0.69	$0.0007	$0.0069
zkSync	$0.09	$0.22	$0.0009	$0.0022
Polygon Hermez	$0.25	-	$0.0025	-
Optimism	$0.37	$0.54	$0.0037	$0.0054
Arbitrum One	$0.53	$0.74	$0.0053	$0.0074
Data sourced from L2fees.info		March 17, 2022		

Security

There are many different types of security: smart contract security, economic security, network security, etc. Today, the network that has been free of attacks for the longest time and is the most resistant is the Ethereum network, so solutions building on top of it are preferred over separate networks with their economic security guarantees. The most mature ecosystem is the EVM in terms of smart contract security. Our contracts are written in Solidity at the present moment and are undergoing an audit by Sigma Prime; this is to ensure that there are no possible exploits of our infrastructure. As an organization, we should audit different networks where we could deploy these contracts to minimize attack vectors and risk surface area.

If we want to optimize for security, most alt L1s excluding data availability only layers like Celestia or Polygon Avail should not be considered valid solutions. They are nowhere close as secure as rollups or honest minority assumption constructions Arbitrum AnyTrust / zkSync zkPorter.

Scalability

To support millions and potentially billions of users one day, we need to watch for the solution that provides the highest scalability assurances within our requirements space. Modular blockchains and L2s are the dominant solutions as rollups (optimistic or zero-knowledge), and off-chain data availability solutions like validiums or AnyTrust chains can provide the best scalability without compromising on security or decentralization. A great property of rollups/validiums/AnyTrust is that they are the most scalable solutions without sacrificing decentralization or security.

An important note in this area is that most of these architectures are not as mature as sidechains/commit chains like Polygon PoS or Gnosis Chain or some longer-lived EVM-compatible alt L1s like BSC or Fantom. The most mature construction is optimistic rollups (ORUs), where there are two serious contenders: Optimism and Arbitrum One. Generalized zero-knowledge rollups (ZKRUs) are mostly in the R&D phase. They are not yet ready for production use, so it is wise to disregard them as a possible solution for immediate use for Alongside.

Decentralization of infrastructure

L2s on Ethereum, although decentralized in theory, are not fully decentralized as they currently stand. ORU Sequencers (= nodes that execute all of the transactions on the network and relay + commit the state change to L1) are operated by the same teams that built them: OptimismPBC for Optimism and OffChain Labs for Arbitrum One. Another core piece of ORU infrastructure is fraud provers which check for invalid transitions and revert the state to the latest commit in the case of fraud. Arbitrum One has had a live fraud prover system for almost a year now, but OffChain Labs operates both provers. Optimism's fraud prover system (Cannon) has not yet been deployed to the mainnet as they have changed the architecture of the network a few times, and the prover needs to be appropriately adjusted. However, I learned that it would be live in the coming months, thanks to my recent visit to Amsterdam (I'm good friends with the Optimism team and the teams behind most scalability solutions), so we might get alpha early).

All of these infrastructural pieces are being decentralized. However, it may take some time, which is a trust assumption we would assume if we were to deploy on these networks.

Good tooling

This requirement refers to all of the tools that blockchain developers have access to. In our context, it is Solidity + EVM for execution. Optimism is EVM-equivalent, so a contract bytecode is 1-1 to regular Ethereum bytecode, and all of the tools work out of the box. Arbitrum's virtual machine (AVM) is almost identical to the EVM; differences are detailed here, but the tooling works just as well as on Optimism.

As zero-knowledge rollups and their development environments mature, it might be worth switching to a different execution target like Starknet's Cairo VM or zkSync's LLVM (or any other execution target). The following 2-3 years will be full of experimentation, and we need to position ourselves to share in the upside while staying true to our mission.

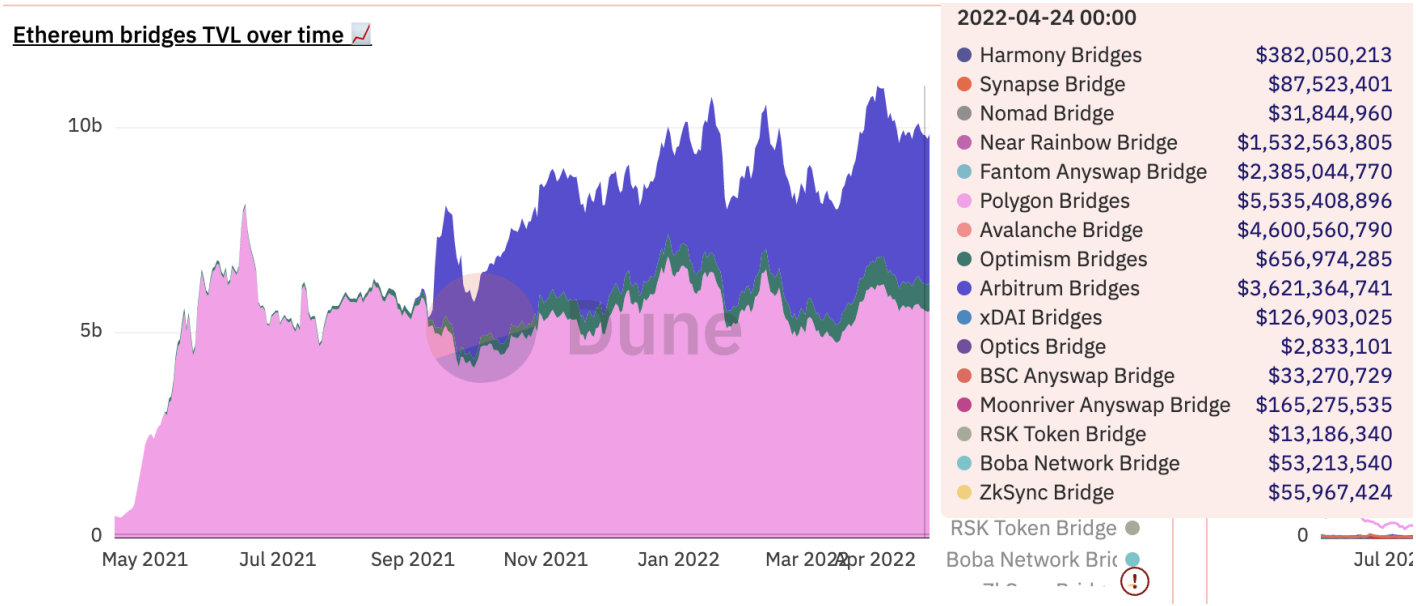
Value alignment

- core crypto values (trustless, immutable, decentralized, permissionless, individual sovereignty, ...)
- ease of use
- long-term oriented
- optional: public goods, regenerative cryptoeconomics, ...
- TBD

Interoperability

This is one of the essential requirements for our use case. We need the network we deploy on to have access to as many DeFi primitives as possible, deep liquidity pools, necessary tooling like multisigs, DAO tooling, wallet and CEX support, community awareness, etc.

In this area, Arbitrum is the clear winner. Their business development team has been able to strike meaningful partnerships and lobby within the governance of several DAOs and projects to deploy on top of them. Another important factor contributing to this is the private (whitelist) mainnet that Optimism had in the early stages. In contrast, Arbitrum One was open to the broader public a few weeks sooner. Most major CEXes have announced L2 support or support them already. Alternatively, users can leverage intermediate CEX liquidity solutions like LayerSwap.



TVL:

- Polygon PoS: $5.5B

Name	Chains	1d Change	7d Change	1m Change	TVL	Mcap/TVL
1 AAVE (AAVE)		-1.36%	-6.49%	-25.93%	$894.31m	2.54787
2 Quickswap (QUICK)		-0.82%		-13.28%	$747.14m	0.09912
3 Curve (CRV)		-4.29%	-5.48%	-8.28%	$368.15m	2.56014
4 Stargate (STG)		-3.17%	-22.89%	-51.16%	$246.95m	
5 SushiSwap (SUSHI)	+4	-0.70%			$214.62m	2.68191
6 Balancer (BAL)		-2.76%	-14.13%	-21.88%	$196.25m	0.78045
7 QiDao (QI)		+1.25%	-2.29%	-5.17%	$138.56m	0.36473
8 Uniswap (UNI)				-13.13%	$126.94m	29.37898
9 Beefy Finance (BIFI)	+4	-2.73%	-4.60%	-9.56%	$119.29m	0.93262
10 Klima DAO (KLIMA)		-0.56%	-4.93%	-4.15%	$71.13m	1.12702
11 Arrakis Finance		+0.41%	+28.56%		$51.22m	
12 Synapse (SYN)	+4	+2.65%	+6.03%	+9.09%	$48.52m	11.43404
13 AAVE V3 (AAVE)		+9.98%	+18.67%	+69.49%	$34.71m	

- Optimism: $0.66B

Name	Chains	1d Change	7d Change	1m Change	TVL	Mcap/TVL
1 Synthetix (SNX)		-0.96%	-2.63%	+2.78%	$211.59m	5.81689
2 Uniswap (UNI)				-3.92%	$44.01m	84.73903
3 Perpetual Protocol (PERP)		+0.22%	-1.37%	+32.18%	$40.82m	6.29687
4 Lyra (LYRA)		+2.54%	+3.15%	-0.93%	$39.92m	0.52375
5 Stargate (STG)		-0.92%	-10.41%	+4.98%	$37.59m	
6 Synapse (SYN)	+4	+2.17%	-2.40%	-6.82%	$36.27m	15.29579
7 Hop Protocol		-0.40%	+7.78%	+8.92%	$13.21m	
8 ZipSwap (ZIP)		-0.68%	-10.51%	+23.88%	$11.73m	
9 Curve (CRV)		-4.17%	+45.35%	+2041%	$11.14m	84.63371
10 Arrakis Finance		+0.20%	-1.40%	+42.73%	$8,025,922	
11 AAVE V3 (AAVE)		-19.45%	+54.66%	+281%	$6,787,108	

- Arbitrum: $3.3B

Name	Chains	1d Change	7d Change	1m Change	TVL	Mcap/TVL
1 SushiSwap (SUSHI)	+4	+0.60%			$514.07m	1.11969
2 GMX (GMX)		+0.69%	+0.21%	+9.92%	$251.99m	0.88036
3 Curve (CRV)		+0.47%	+0.01%	+8.52%	$230.8m	4.08363
4 Stargate (STG)		+0.07%	-15.19%	-28.54%	$220.88m	
5 Synapse (SYN)	+4	+0.23%	-0.48%	-0.38%	$147.04m	3.77312
6 dForce (DF)		+0.25%	-0.84%	-0.97%	$136.3m	0.20663
7 Uniswap (UNI)				-2.83%	$92.12m	40.48271
8 Abracadabra (SPELL)		-0.75%	-4.81%	-13.57%	$70.99m	4.58052
9 Dopex (DPX)		-0.15%	-11.50%	-24.19%	$68.48m	3.0024
10 Balancer (BAL)		-0.49%	-26.65%	-41.10%	$50.02m	3.06195
11 Hop Protocol		+3.17%	-0.65%	-5.74%	$23.94m	
12 Saddle Finance (SDL)		-1.03%	+3.41%	-12.86%	$23.59m	
13 Sperax USD (USDs)		+0.24%	-0.80%	-2.10%	$22.76m	5.40313
14 Vesta Finance (VSTA)		+1.28%	-1.32%	-5.59%	$19.91m	0.19678
15 Beefy Finance (BIFI)	+4	+0.46%	-9.48%	-14.10%	$16.35m	6.80403

Currently, Polygon PoS would be the most sound deployment solution regarding access to DeFi primitives. However, it doesn't meet security, decentralization, and scalability concerns unless the team plans to turn the PoS commit chain into a rollup/validium (there's no public information available on this, only speculation).

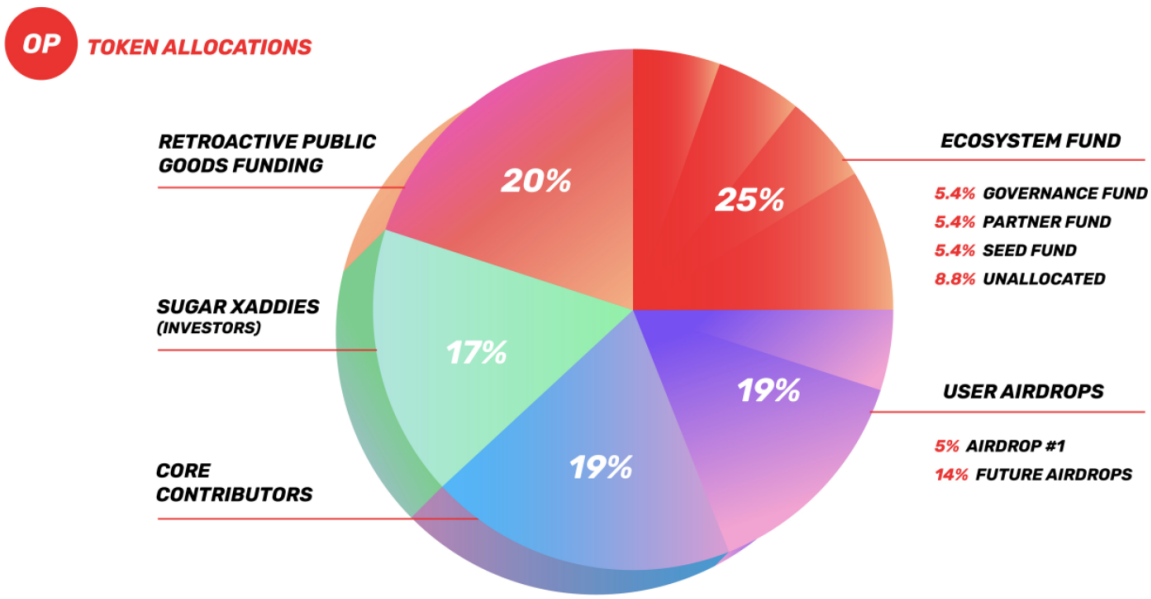
The second best is Arbitrum, and the third is Optimism (although with the newly announced token, both Arbitrum and Optimism will likely even out).

Incentives

If we are to deploy on any of these networks, there are huge grants offered to the teams that attract the most TVL / adoption to the chain. Arbitrum (most likely) and Optimism will airdrop tokens to the protocols that drive the most adoption.

In terms of incentives alone, we could likely get more significant rewards from teams like Polygon or even from funds like Avalanche DeFi fund, etc. Polygon PoS would be the best compromise in this regard, but their ZKRU solutions (Miden, Zero, Hermez) are still some time away from mainnet deployment unless we use the less secure and less decentralized PoS chain.

Allocations at a glance



Flexibility

Questions to think about in this area:

- **Q:** If the Alongside protocol wanted to pivot, how complex would it be?

- **A:** Right now, it is very unclear how this might go as there are hardly any examples of this that have already happened. My educated guess is a mix of liquidity mining incentives, infrastructural restructuring and refactoring, and education and spreading awareness of the change.
- **Q:** Can the scalability solution on top of which Alongside is deployed pivot? How realistic is this possibility?
  A: Each solution is different, but optimistic rollup teams have told me that their infrastructure is modular enough to allow for the integration of validity proofs (ZK) into their system with the potential of a complete overhaul (given the approval of governance - token holders)
- Long term:
  - We can change tech stack
    - zkSync (LLVM)
    - Starknet (Cairo)
    - other exotic VMs (TBD)

Conclusion

I believe that Optimism has the best balance of all the requirements above and Arbitrum is closely behind. However, if we want to optimize for funding Polygon PoS will help us the most with the initial liquidity bootstrapping. Although building on Arbitrum and Optimism and getting ecosystem rewards might be a more lucrative endeavor long term.